Pré-Print de Boris Beaude, 2015, « La vulnérabilité réticulée », in *La cyberdéfense. Quel territoire, quel droit ?, dir. Amaël Cattaruzza et Didier Danet,* Economica, *pp. 60-70.*

> *« We know hackers steal people's identities and infiltrate private email. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy. »*
>
> Barack Obama, *State of the Union Address*, 12 février 2013

La vulnérabilité réticulée

Boris Beaude

Dans son discours sur l'État de l'Union du 12 février 2013, le président des États-Unis Barack Obama dénonça ouvertement les risques accrus de piratage informatique et l'importance de s'en prémunir activement. Ces trois dernières années, les révélations relatives à la vulnérabilité des dispositifs informatiques furent si nombreuses, qu'elles suscitèrent des réactions de plus en plus vives, qui engagent à un renouvellement de notre conception de la sécurité.

En plus d'une apparente généralisation de cette vulnérabilité inédite, les attaques informatiques sont d'autant plus déstabilisantes qu'elles reposent sur les propriétés spécifiques des réseaux de télécommunication numériques, qui se distinguent très significativement d'autres formes de vulnérabilité plus conventionnelles pour lesquels des dispositifs techniques spécifiques furent développés.

En particulier, la frontière[1] semble être particulièrement affectée par ce type d'attaques. Elles s'appuient en effet sur un système technique qui n'est structurellement pas conforme au découpage territorial du Monde selon les États-nations. En changeant l'espace, Internet a en effet démultiplié les relations entre des espaces autrement disjoints, créant du contact où il y avait de l'écart. En faisant du Monde un lieu, ce sont les lieux du Monde qui se trouvent affectés par le risque d'être vulnérables à des atteintes réticulaires à leur intégrité.

Dès lors, quel peut être l'espace légitime du politique susceptible d'organiser la spatialité spécifique d'Internet ? Cet espace présente certes des opportunités remarquables pour l'humanité, mais il réduit tout autant la souveraineté et la maîtrise de ses composantes particulières.

[1] La frontière est ici appréhendée dans sa dimension politique, comme interface entre deux territoires distincts.

Une vulnérabilité généralisée

Le 28 mai 2013, nous apprenions dans un rapport du Defense Science Board destiné au Pentagone que les plans de nombreuses armes américaines avaient été dérobés lors d'une attaque informatique. La Chine était pressentie comme le très probable initiateur de cette attaque. Une attaque particulièrement préoccupante dès lors que ces plans concernaient des dispositifs hautement stratégiques, tels que le prototype du futur F35, le F18, les missiles Patriot, les radars Aegis, ou l'hélicoptère hybride V-22 Osprey[2].

Cet incident fut considéré comme une attaque organisée, qui coïncide avec la révélation de l'existence d'une importante unité de piratage située dans la banlieue de Shanghai. La société de sécurité privée Mandiant annonçait en effet en février 2013 qu'un groupe de hackers réparti sur les douze étages d'un immeuble affilié à l'Armée populaire de libération opérait des attaques depuis au moins 2006, subtilisant les données de 141 entreprises, dont 115 étaient américaines. La même entreprise révéla que Coca-Cola faisait partie des victimes et que l'attaque coïncida avec l'échec de la tentative d'acquisition de China Huiyuan Juice Group.

Ces révélations particulièrement sensibles s'inscrivent dans le prolongement de la radicalisation des États-Unis à l'égard des attaques informatiques, particulièrement bien exprimées en juin 2011 par Leon Panetta. Alors directeur de la CIA, il attira l'attention sur le risque d'un Pearl Harbor numérique, avant de devenir ministre de la Défense des États-Unis. Toutes les composantes de ce qui est à présent communément qualifié de cyberguerre étaient réunies (*cyber warfare*).

À cette même période, le Pentagone déclara officiellement que toute attaque informatique serait dès lors considérée comme un acte de guerre auquel les États-Unis pourraient répondre par une attaque militaire, informatique, mais aussi conventionnelle[3]. Cette réaction semble répondre à une généralisation des attaques informatiques à des composantes de plus en plus nombreuses de la société. En plus des attaques importantes dont la Géorgie et l'Iran furent les victimes en 2008 et en 2010, et des révélations de la société Mandiant qui recouvrent la plupart des domaines de l'activité économique (aérospatial, recherche, transports, énergie, finance...), les déclarations de nombreuses entreprises et gouvernements ne cessent de se multiplier, tel un aveu partagé d'impuissance à l'égard d'un phénomène dont l'ampleur est insaisissable.

Des déclinaisons de Stuxnet ont en effet été utilisées pour affecter des installations pétrolières du Moyen-Orient et des banques libanaises, le Ministère des Finances et l'Élysée ont reconnu avoir été l'objet de surveillance lors de l'organisation du G20 et des entreprises, de plus en plus nombreuses, admettent être sujettes à des attaques relativement importantes qui affectent non seulement les informations relatives à leurs clients, mais aussi leur propre activité. Heartland Payment Systems, dont 130 millions d'informations relatives à des cartes de crédit ont été

[2] Ellen Nakashima, «Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies», *The Washington Post*, 28 mai 2013.
[3] Siobhan Gorman And Julian E. Barnes, «Cyber Combat: Act of War. Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force», The Wall Street Journal, 31 mai 2011.

dérobées, mais aussi Evernote, Living Social, Ubisoft ou Playstation Network, dont plus de 50 millions de comptes ont été piratés, incarnent parfaitement ce qui s'apparente à une incertitude grandissante quant à la sécurité des systèmes informatiques. Plus récemment, Adobe fut non seulement affecté par la subtilisation des informations relatives à 44 millions de clients, mais aussi du code source de la plupart de leurs logiciels, sans être en mesure de connaître l'ampleur précise de cette attaque.

Enfin, les déclarations répétées de nombreux média nord-américain dont les ordinateurs ont fait l'objet de surveillance[4] et de Google dont de nombreux comptes Gmail de dissidents chinois furent compromis soulignent ce qui s'apparente à la fin du secret des sources et des investigations au profit des plus puissants. Comprendre l'émergence d'une telle vulnérabilité suppose de mieux en comprendre la spatialité inédite et les propriétés spécifiques des dispositifs d'interaction numériques. Il est à présent manifeste que ces atteintes à la souveraineté affectent non seulement les gouvernements, mais aussi les entreprises, les associations et les individus, dans des proportions inimaginables avec des moyens plus conventionnels.

Une vulnérabilité inédite

Ce qui apparaît, après des années d'atteintes à l'intégrité des dispositifs connectés à Internet, c'est essentiellement l'inadéquation des cadres conventionnels qui organisent et régulent la réaction adéquate à un acte de guerre. Porter atteinte à des dispositifs informatiques et en compromettre les données ou le fonctionnement semble relever d'une atteinte ordinaire à des biens situés, qui autorisent une riposte appropriée. Pourtant, s'il s'agit de « guerres », conformément à l'infléchissement linguistique opéré ces dernières années, il s'agit de guerres d'une rare discrétion et dont les modes opératoires sont particulièrement insidieux. En particulier, ce type d'attaque se caractérise par un ensemble d'attributs qui, ensemble, composent le caractère inédit de cette vulnérabilité. Les attaques numériques présentent en effet la particularité d'être invisibles, complexes, d'une rapidité considérable et d'origines indéterminées.

L'invisibilité est en effet l'une des particularités de ce type d'attaque. La prise de contrôle d'une machine, la surveillance des données qui s'y trouvent et la mise en place de dispositifs susceptibles d'en affecter le fonctionnement peuvent être totalement invisibles. Ce principe repose sur la particularité des modes d'interaction immatériels, qui exigent des dispositifs spécifiques pour en identifier la présence. Une tension se crée alors entre les moyens de ne pas être observable et les moyens de l'observation. L'art de la guerre numérique est en cela aussi un art de l'invisibilité, au même titre que lors d'attaques plus conventionnelles, mais dans des proportions nettement plus remarquables.

La complexité est l'une des autres composantes des attaques informatiques. Ces attaques exploitent des dispositifs d'une rare complexité, dont la maîtrise est très inégalement partagée. Il n'est pas nécessaire de comprendre l'ensemble du fonctionnement d'un F18 pour le voir arriver.

[4] En particulier The New York Times, The Washington Post, The Wall Street Journal et CNN début 2013.

L'informatique est un environnement plus complexe que la terre, la mer et l'air, démultipliant les modes de transmission et les vulnérabilités, un programme pouvant se dissimuler dans une musique, une vidéo, un fichier PDF ou un autre programme. La prise de contrôle d'une machine ou la surveillance d'un réseau peut ainsi se faire totalement à l'insu de ses utilisateurs, en profitant de failles délibérées ou non, qui dispensent même d'une négligence de la cible.

La rapidité, associée à l'invisibilité et à la complexité des attaques, participe elle aussi de cette vulnérabilité spécifique, la prise de contrôle d'une machine pouvant s'effectuer presque instantanément depuis n'importe quelle partie du Monde. L'organisation structurée des ondes électromagnétiques proposée par Internet autorise en effet des vitesses proches de celle de la lumière, sans commune mesure avec le déplacement d'armes plus conventionnelles.

Enfin, la composante probablement la plus importante de cette vulnérabilité inédite tient à la difficulté particulière à identifier la source d'une attaque. Alors qu'une arme conventionnelle dispose de caractéristiques matérielles et d'une trajectoire plus clairement identifiables, une attaque informatique peut être invisible, rapide et d'une complexité telle qu'il ne soit pas possible d'en identifier clairement la source. Ce constat tient précisément à la faiblesse des dispositifs informatiques dont la vulnérabilité est de plus en plus systémique, dès lors que les attaques peuvent être perpétrées par l'intermédiaire de nombreuses machines à l'insu de leur propriétaire. La simple reconnaissance de la possibilité d'une attaque suppose que toute machine peut en faire l'objet et que la source de l'attaque peut en cela être elle même la victime d'une attaque antérieure et coordonnée. C'est précisément ce raisonnement qui fut mobilisé par la Russie à l'égard de la Géorgie en 2008 ou de la Chine à l'égard des États unis à de très nombreuses reprises. Le principe des attaques distribuées sur un nombre considérable de machines dont le contrôle n'est plus assuré par leur propriétaire fut parfaitement illustré par le botnet Citadel, qui contrôlait plus de 5 millions d'ordinateurs avant d'être démantelé dans le cadre d'une importante collaboration entre Microsoft, le FBI et les gouvernements de plus de 80 pays[5].

Enfin, les révélations récentes de Wikileaks dans le cadre des Spy Files[6] et de Richard Snowden relatives à la NSA (National Security Agency)[7] ont souligné l'ambiguïté des gouvernements. Le cas de la Libye fut symptomatique de cette ambiguïté, alors que le dispositif de surveillance utilisé par le régime autoritaire de Mouammar Kadhafi fut développé par la société d'ingénierie informatique française Amesys. Par ailleurs, en abusant de leur contrôle auprès de nombreux acteurs de l'économie numérique[8], les États-Unis s'autorisent à surveiller massivement le Monde

[5] Ce botnet fut utilisé pour prélever illégalement de l'argent au détriment des principaux établissements bancaires dont American Express, PayPal, HSBC, Crédit Suisse, Bank of America et Citigroup. Jim Finle, «Microsoft, FBI take aim at global cyber crime ring», *Reuters*, le 5 juin 2013.
[6] http://wikileaks.org/the-spyfiles.html
[7] Cf. l'article de synthèse proposé par le Guardian, principal médiateur de Richard Snowden lors de ces révélations par l'intermédaire du journaliste Glenn Greenwald. Ewen acaskill et Gabriel Dance, «NSA Files : Decoded. What revelations mean for you», *The Guardian*, 1er novembre 2013.
[8] Les États-Unis entretiennent en effet des relations privilégiées avec des opérateurs de services tels que Google ou Facebook, des opérateurs de télécommunication tels de AT&T ou Verizon, des opérateurs de réseaux tels que Level 3 ou des leaders informatiques tels que IBM, Cisco ou Microsoft.

entier, dont des entreprises et des chefs d'État, parmi lesquels les dirigeants de partenaires commerciaux et politiques de premier ordre tel que l'Allemagne.

S'oppose ainsi la résilience considérable d'Internet à des attaques informatiques, l'ensemble du réseau étant d'une rare stabilité, à la vulnérabilité considérable de ses noeuds (routeurs, ordinateurs, téléphones mobiles...) dont les données et le fonctionnement peuvent être manipulés en toute discrétion ou avec la volonté manifeste d'en altérer visiblement l'intégrité. L'extension d'Internet à l'ensemble des pratiques économique et politique expose en cela à des problématiques sécuritaires inédites, qui soulignent la faiblesse des frontières à assurer la souveraineté dont les États-nations se prévalent volontiers. Ce sont en effet tous les noeuds du réseau qui sont concernés par une telle vulnérabilité. Elle expose potentiellement les gouvernements, les entreprises, mais aussi tous les individus, sans exception, dans le Monde entier.

La pertinence de la frontière

Le principe de réponse équilibrée à une cyberattaque énoncé par les États-Unis pose en cela de nombreux problèmes. En cas d'attaque, même majeure, comment avoir l'assurance de son origine géographique ? Comment engager une riposte sans être certain de la cible ? Comment s'assurer de ne pas être instrumentalisé et de ne pas répondre à une attaque dont l'origine est feinte afin qu'elle soit la réelle cible ? Ces questions n'ont pas de solution évidente. Elles soulignent en revanche la problématique de cette vulnérabilité particulière, dès lors que son origine ne peut être certaine !

Néanmoins, les États-Unis énoncent ouvertement s'être dotés de compétences non seulement de défense, mais aussi d'attaque. Stuxnet est probablement le cas le plus emblématique et le plus ambigu de ce mode opératoire[9]. Par ailleurs, le gouvernement chinois est régulièrement dénoncé pour ses attaques coordonnées depuis des espaces clairement identifiés tels que le bâtiment de l'Armée populaire de libération situé dans le quartier de Pudong de la banlieue de Shanghai, un établissement de formation professionnelle de Lanxiang initialement fondé par cette même armée, ainsi que l'Université de Shanghai Jiaotong[10]. Le potentiel des attaques exploitant les failles des dispositifs numériques, particulièrement insidieuses, ne dissipe pourtant pas le risque qu'elles recouvrent dès lors qu'elles se généralisent, que les moyens d'attaques s'officialisent et que la riposte n'en demeure pas moins particulièrement difficile.

C'est pourquoi la compréhension de la nature de cette vulnérabilité exige de reconsidérer pleinement la spatialité spécifique d'Internet et ses relations avec d'autres espaces, dont le territoire. Avec le déploiement d'Internet, c'est en effet la notion même de frontière qui est affectée, ainsi que son effectivité. La frontière se trouve débordée de toute part par un réseau dont les fondements furent précisément élaborés au service de la décentralisation et de la

[9] David E. Sanger, «Obama Order Sped Up Wave of Cyberattacks Against Iran», *The New York Times*, le 1er juin 2012.
[10] John Markoff et David Barboza, «2 China Schools Said to Be Tied to Online Attacks», *The New York Times*, le 19 février 2010.

désintermédiation. La notion de frontière n'y est structurellement pas présente. Ce principe s'inscrit dans un contexte particulier, alors qu'Internet fut élaboré par des ingénieurs et des chercheurs influencés par la cybernétique de l'après Deuxième Guerre mondiale, participant de la contre-culture libertaire qui émergea à partir des années soixante. Le communisme, la religion, mais aussi l'État, étaient dès lors perçus comme des éléments perturbateurs de la libre circulation de l'information, comme des altérations susceptibles de réduire ou d'anéantir le *feed-back* dont les sociétés ont besoin pour être visibles à elles-mêmes et prendre les décisions collectives qui conviennent. En cela, la frontière n'est pas inscrite au sein des protocoles fondamentaux d'Internet, dont la suite TCP/IP constitue un parfait exemple.

Plus généralement, Internet rappelle à quel point la frontière est une construction, une discontinuité active qui, pour être effective, exige des dispositifs symboliques, juridiques et matériels particulièrement sophistiqués. La frontière crée une rupture où il y a souvent de la continuité. Internet nous rappelle que la frontière est une production sociale, contextuelle et fragile. La frontière répond provisoirement à un besoin d'ordonnancement du Monde. Elle définit l'opposition territoriale entre un collectif d'individu et ce qui en constitue une altérité politique, elle oppose un eux à un nous, fragile, mais nécessaire à l'émergence du politique.

Or, Internet est structurellement a-territorial. Il s'inscrit certes dans un dispositif technique matériel, situé et parfaitement territorial, mais son fonctionnement n'est que très indirectement tributaire de ce dispositif. La topologie des liens hypertextes, par exemple, est totalement disjointe de celle du réseau technique sous-jacent. En cela, Internet est un espace mondial à échelle unique, dont toutes les parties ne sont virtuellement qu'à une connexion l'une de l'autre. Pour être effective, cette connexion va mobiliser de nombreux dispositifs intermédiaires, tous situés, mais sans que cela ne soit explicite et perceptible.

De plus, la frontière n'est pas pertinente pour les paquets d'information qui transitent sur Internet. Ces paquets circulent d'un nœud à un autre selon la topologie du réseau et non selon la topographie des territoires. C'est précisément ce potentiel de connexité qui constitue la puissance d'Internet à créer des relations inédites entre les lieux. Cette connexité change très significativement les virtualités de l'espace, en autorisant des pratiques autrement impossibles. C'est pourquoi en changeant l'espace, Internet change aussi la société. C'est aussi pour cela que les vulnérabilités auxquelles nous sommes exposés sont tellement soudaines et inédites.

À présent, la guerre économique et politique s'est adaptée à ce nouvel espace. La connexion est en cela autant de portes ouvertes sur le Monde, autant d'opportunités de créer de nouvelles relations sur de vastes étendues, mais elle est aussi autant de portes ouvertes sur la vie privée, sur le secret économique et sur le secret politique. Cette connexion constitue en effet une ouverture redoutable sur des infrastructures stratégiques, elles-mêmes de plus en plus informatisées et de plus en plus connectées.

Cette dissipation fonctionnelle de la frontière est en cela particulièrement problématique, dès lors qu'elle demeure une composante décisive du politique. Elle structure l'organisation différentielle des valeurs en proposant une subdivision partielle du Monde en parties qui répondent à un

ensemble de principes communs de coexistence. La frontière assure en cela un équilibre provisoire entre des sociétés d'individus et suppose de convenir des conditions nécessaires pour passer d'une société à une autre. La frontière définit en cela la limite au-delà de laquelle les règles, les droits et les devoirs qui organisent la coexistence changent, parfois radicalement. C'est pourquoi les États-nations œuvrent de plus en plus à recouvrer sur Internet la souveraineté dont ils se sentent légitimes et qu'ils considèrent avoir largement perdue. Chacun souhaite pouvoir y appliquer les règles qui organisent leur coexistence territoriale, opposant à la mondialité d'Internet la nationalité de leur droit.

Le blocage du site Copwatchnrd-idf.org depuis la France en octobre 2011, les représentations différentes des frontières de la Chine sur Google Map selon les pays, l'impossibilité d'accéder à Facebook depuis l'Iran ou l'impossibilité de disposer d'un accès à la version américaine de Netflix depuis la France résument bien la pluralité des logiques d'imposition de frontières où il n'y en a initialement pas.

Au nom de la sécurité, de la diplomatie, de la stabilité sociale ou de la propriété intellectuelle, les raisons d'ériger des frontières sur Internet sont néanmoins multiples, souvent légitimes et de plus en plus évidentes. Au nom du contrôle de ce qui advient sur cet espace, la plupart des pays revendiquent ainsi de plus en plus activement de pouvoir y faire respecter les règles qui régissent le vivre ensemble auprès de leurs citoyens respectifs.

Construire l'effectivité de la frontière sur Internet exige pourtant de contrevenir à son fonctionnement et plus généralement à ce qui est communément appelé la neutralité du Net. Ce principe suppose en effet que les paquets d'informations soient traités indifféremment de leur origine, de leur destination et de leur contenu. Or, l'application du droit à cet espace exige au contraire de prendre connaissance, pour chaque paquet, de leur origine, de leur destination et de leur contenu, au même titre que ce qui est à l'œuvre entre pays qui ne disposent pas d'une zone de libre-échange ou de libre circulation.

Internet et l'espace légitime du politique

La neutralité du Net est à présent un principe plus politique que technique, de moins en moins partagé et de plus en plus discuté. Elle suppose l'adéquation parfaite entre Internet et le Monde, mais aussi la cohérence politique de l'humanité. La neutralité du Net exclut en effet toute politique d'Internet, puisqu'elle exclut le traitement différentiel de ses parties. Cette option radicale est néanmoins un projet politique puissant, qui fait d'Internet un espace commun pour l'humanité, et du Monde l'espace de la société correspondante.

Or, les attaques numériques sophistiquées, la surveillance généralisée, mais aussi l'ensemble des mesures qui encadrent de plus en plus la liberté d'expression et la propriété intellectuelle, révèlent à quel point la mondialité d'Internet s'effondre chaque jour un peu plus. Nous assistons à un double effondrement de l'échelle mondiale. D'une part, Internet est de moins en moins un espace de libre échange qui suppose des valeurs communes entre l'ensemble de ses utilisateurs. D'autre part, il tend à être divisé conformément à l'organisation territoriale du politique.

La neutralité du Net est en effet progressivement anéantie par les dispositifs de surveillance, qui supposent d'analyser précisément le contenu, l'origine et la destination de chaque paquet. Le principe de riposte équilibrée ne fera qu'accroître le besoin de certitude quant à la circulation des informations sur Internet, afin de pouvoir trouver l'origine ultime d'une attaque et de conforter le processus de décision qui motiverait une riposte conventionnelle et d'en assumer les conséquences.

Aussi, afin d'assurer la sécurité de l'ensemble des dispositifs informatiques connectés, la tentation est de plus en plus grande de transposer la territorialisation de l'espace légitime du politique sur Internet, en y réintroduisant les frontières plus rigoureusement. L'évolution des protocoles et la diffusion actuelle de l'IPv6 (version 6 de l'Internet Protocol) permettront dans un avenir relativement proche d'appliquer plus strictement un contrôle des paquets[11] d'information aux frontières, au même titre que toutes autres réalités sociales, matérielles ou immatérielles.

La vulnérabilité, pourtant, restera immense. La visibilité, dans un tel domaine, reste en effet très relative à la compétence dont le surveillant dispose pour en identifier la nature et le fonctionnement. Aussi, Internet peut être un mode de propagation, dont le vecteur initial aurait été infecté par des moyens plus conventionnels, tels qu'une clé USB, à l'image de l'attaque de 2009 contre les centrifugeuses iraniennes de Natanz opéré par Stuxnet.

La puissance de cette vulnérabilité devrait finalement asseoir plus encore le pouvoir de ceux qui maîtrisent le numérique, selon la pluralité de ces composantes. Être maître dans l'art de la cyberguerre suppose en effet de disposer de compétences multiples et systémiques, dont l'ensemble des parties constitue un environnement total qui ne tolère aucune faille. La cyberguerre suppose en effet de maîtriser les protocoles (TCP/IP, DNS...), les infrastructures (backbones, FAI...), les services (réseaux sociaux, moteurs de recherche...), les dispositifs (routeurs, smartphone, ordinateurs...) et les logiciels (systèmes d'exploitation, navigateurs...). C'est pourquoi les États-Unis disposent d'une puissance considérable, dont la surveillance est une arme préventive particulièrement puissante, qui transgresse les frontières jusque dans les moindres recoins du Monde. C'est aussi pourquoi les moins puissants acceptent volontiers des partenariats qui assoient plus encore le pouvoir des États-Unis, afin de profiter de cette force de surveillance, de dissuasion et de frappe. C'est enfin pourquoi les moins puissants le sont moins encore, le numérique s'ajoutant à l'ensemble de leurs vulnérabilités existantes.

Mais à un tel « jeu », les États-Unis, mais aussi l'ensemble des puissances militaires conventionnelles, ne seront pas nécessairement les gagnants. La réplique des armes numériques, l'utilisation des failles et la dissimulation sont beaucoup plus aisées dans ce contexte qu'elles ne l'étaient antérieurement. Or, les pays les plus vulnérables de telles attaques sont essentiellement ceux qui sont les plus informatisés et les plus connectés. La partition d'Internet en une multitude d'intranets nationaux et le développement d'armes numériques sophistiquées constituent en cela un risque dont les puissances qui en seront à l'origine en seront probablement les plus grandes

[11] Ce terme renvoi à la *commutation de paquets* utilisée pour transettre l'information par Internet.

victimes. Car une fois encore, la tentation est grande pour les États-nations de ne pas voir que le Monde est un problème pour leur souveraineté, mais aussi une solution. La partition est provisoirement légitime, mais elle expose à une altérité qui ne disparaît pas avec les frontières. Et lorsque la puissance est numérique, elle circule rapidement, se duplique rapidement, se transforme rapidement, et peut être dévoyée tout aussi rapidement contre son initiateur.

Bibliographie

Beaude, Boris, *Internet. Changer l'espace, changer la société*, FYP Éditions, 2012.

Benkler, Yochai, *The Wealth of Networks: How Social Production Transforms Markets And Freedom*, Yale University Press, 2006.

Castells, Manuel, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press, 2001.

Cerf, Vinton, « Nous devons défendre la liberté sur Internet », *Le Monde*, 4 décembre 2012.

Doueihi, Milad, *Pour un humanisme numérique*, Seuil, 2011.

Durand, Marie-Françoise, Jacques Lévy et Denis Retaillé, *Le monde, espaces et systèmes*, Presses de la Fondation nationale des sciences politiques, 1992.

Elias, Norbert, *La Société des individus*, Fayard, 1991.

Joel N. Gordes et Michael Mylrea, «A new security paradigm is needed to protect critical US energy infrastructure from cyberwarfare», *Foreing Policy Journal*, 14 september 2009.

Habermas, Jürgen, *Après l'État-nation: une nouvelle constellation politique*, Fayard, 2000.

Lessig, Lawrence, *Code and other laws of cyberspace*, Basic Books, 1999.

Lévy, Jacques, *L'espace légitime*, Presses de la Fondation nationale des sciences politiques, 1994.

Lussault, Michel, *L'avènement du Monde. Essai sur l'habitation humaine de la Terre*, Seuil, 2013.

Macaskill, Even et Gabriel Dance, « NSA Files : Decoded.What the revelation mean for you», *The Guardian*, octobre 2013.

Musso, Pierre, *Télécommunications et philosophie des réseaux: la postérité paradoxale de Saint-Simon*, Presses universitaires de France, 1997.

Popper, Karl, *La société ouverte et ses ennemis: Tome 1 et 2*, Éditions du Seuil, 1979.

Schafer, Valérie et Hervé Le Crosnier, *La neutralité de l'Internet: un enjeu de communication*, Paris, CNRS Editions, 2011.

Schmidt, Eric von et Jared Cohen, *The New Digital Age: Reshaping the Future of People, Nations and Business*, Hodder And Stoughton Limited, 2013.

Turner, Fred, *From Counterculture to Cyberculture*, The University of Chicago Press, 2006.

Wiener, Norbert, *The human use of human beings: cybernetics and society*, Da Capo Press, 1950.

Wu, Tim, « Network Neutrality, Broadband Discrimination », *Journal of Telecommunications and High Technology Law*, vol. 2, p. 141, 2003.